The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
8/11/2010

SUBJECT:
Vulnerability in Windows Movie Maker Could Allow Remote Code Execution (MS10-050)

OVERVIEW:
A vulnerability has been discovered in Windows Movie Maker which could allow an attacker to take complete control of an affected system. Windows Movie Maker is a video editing application available for Microsoft Windows, which is installed by default on Windows XP and Vista systems. This vulnerability could allow remote code execution if a user opens a specially crafted Windows Movie Maker project file (.MSWMM). The file may be received as an email attachment, on removable media, or downloaded via the web. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs, view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition.

SYSTEMS AFFECTED:

Windows XP SP3
Windows Vista

RISK:

Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Home users: High

DESCRIPTION:
A vulnerability has been identified in Microsoft Windows Movie Maker that could allow an attacker to take complete control of an affected system. This vulnerability exists because of the way Microsoft Windows Movie Maker parses Movie Maker project files (.MSWMM). Specifically, this issue arises because Microsoft Windows Movie Maker does not perform sufficient boundary checks when parsing strings in maliciously crafted Movie Maker project files. This results in a buffer overflow condition that could allow for remote code execution if successfully exploited by an attacker.

This vulnerability can be exploited via an email attachment or through the Web. In the email based scenario, the user would have to open the specially crafted Movie Maker project file as an email attachment. In the Web based scenario, a user would have to open a specially crafted media file that is hosted on a website. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Consider blocking .MSWMM files at the network perimeter.
- Consider removing the Movie Maker .MSWMM file association.
- Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.

REFERENCES:

Microsoft:
http://www.microsoft.com/technet/security/Bulletin/MS10-050.mspx

VUPEN:
http://www.vupen.com/english/advisories/2010/2047

Secunia:
http://secunia.com/advisories/38931/

Security Focus:
http://www.securityfocus.com/bid/42268

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2564